ISSUE NO.24 01.09.2026

FINANCIAL CRIMES WATCH

CLARITY ACT: A NEW FRAMEWORK IN COMBATING FINANCIAL CRIMES

The Digital Asset Market Clarity Act ("**CLARITY Act**"), which is currently progressing through the legislative process, primarily seeks to establish a regulatory framework for the digital asset market in the United States, while also introducing significant changes in the area of financial crime prevention and enforcement. The bill expands anti-money laundering and countering the financing of terrorism ("**AML/CFT**") obligations by bringing certain digital asset intermediaries within the scope of the Bank Secrecy Act ("**BSA**"); expressly provides for the use of blockchain analytics tools in transaction monitoring; enables suspicious digital asset transactions to be temporarily held under certain circumstances; and strengthens the powers of the U.S. Department of the Treasury to address financial crime risks arising from offshore actors and cross-border digital asset flows.

In this way, the CLARITY Act seeks to integrate the digital asset market more closely into the existing U.S. financial system, not only from a market regulatory perspective, but also in terms of the prevention, detection, and investigation of financial crime.

I. BSA and AML/CFT Framework for Digital Asset Intermediaries

The CLARITY Act brings digital commodity brokers, digital commodity dealers, and digital commodity exchanges that are registered or required to register and permit direct customer access within the definition of a "*financial institution*" for purposes of the BSA. Accordingly, the U.S. Department of the Treasury, acting through the Financial Crimes Enforcement Network ("**FinCEN**"), is required to establish requirements tailored to the size and complexity of these entities and their activities. Under this framework, such entities will be required to establish AML/CFT programs incorporating risk assessments, internal policies and controls, a designated compliance officer, employee training, and an independent audit function; maintain transaction records; monitor and report suspicious activity; and implement effective customer identification and verification programs and customer due diligence procedures.

The bill also expressly provides that appropriate distributed ledger analytics may be used in monitoring suspicious activity and requires covered entities to comply with U.S. sanctions laws and regulations administered by the Office of Foreign Assets Control *(OFAC)*.

II. Temporary Holds on Suspicious Digital Asset Transactions

The CLARITY Act permits certain digital asset transactions to be temporarily held as part of efforts to combat financial crime. Covered entities may impose a hold for up to 30 days where they reasonably believe that a transaction, conversion, or withdrawal is related to unlawful activity or where they receive a qualified written request from an authorized law enforcement agency concerning a specific wallet, address, account, or transaction. This period may be extended for an additional 150 days upon a written request from a law enforcement agency, bringing the total period to up to 180 days. Covered entities are also provided with protection from liability against certain legal claims in respect of temporary holds implemented in good faith and in compliance with the applicable requirements. In addition, documentation relating to the basis for the temporary hold must be retained for three years and made available to the competent authorities upon request.

III. Fraud Prevention Measures for Digital Asset Kiosks

The bill provides for various measures aimed at reducing fraud risks in transactions conducted through digital asset kiosks and crypto ATMs. In this context, operators are required to establish policies and procedures for fraud prevention, designate a compliance officer responsible for these processes, and establish mechanisms for communication with law enforcement agencies. Clear pre-transaction warnings to customers regarding fraud risks and the application of transaction amount and time restrictions to certain transactions by new customers are also among the preventive measures contemplated.

The CLARITY Act also places particular emphasis on the analysis of transactions on the blockchain. Operators are required to use distributed ledger analytics to prevent digital assets from being sent to wallets known to be associated with fraudulent activity and to detect transaction patterns indicative of fraud or other illicit activities.

IV. Financial Crime Measures for Cross-Border Activities

The CLARITY Act provides for additional mechanisms to address offshore stablecoins and digital asset transactions involving foreign actors as part of efforts to combat financial crime. In this context, the U.S. Department of the Treasury is required to periodically assess the illicit finance risks posed by certain offshore stablecoins connected to the U.S. financial system, the controls implemented by issuers to address such risks, the volume of transactions associated with illicit finance, and their relationship with the U.S. financial system. In addition, the special measures under the BSA are expanded to allow the U.S. Department of the Treasury to prohibit or impose conditions on certain transmittals of funds involving foreign jurisdictions, foreign financial institutions, or certain classes of transactions found to be of primary money laundering concern in connection with illicit finance through the use of digital assets.